

Министерство науки и высшего образования Российской Федерации  
ФГБОУ ВО «Алтайский государственный университет»  
международный институт экономики, менеджмента и информационных  
систем

Кафедра прикладной информатики в экономике, государственном и  
муниципальном управлении

**ФОНД  
ОЦЕНОЧНЫХ СРЕДСТВ**

**по дисциплине  
«Технологии информационной безопасности»**

27.03.03. Системный анализ и управление  
«Системный анализ и управление экономическими системами»

Разработчик:  
к.ф.-м.н., доцент кафедры  
прикладной информатики в  
экономике, государственном и  
муниципальном управлении



/О. В. Журенков/

Барнаул, 2020

---

**Визирование ФОС для исполнения в очередном учебном году**

Фонд оценочных средств пересмотрен, обсуждён и одобрен для исполнения в 2020–2021 учебном году на заседании кафедры прикладной информатики в экономике, государственном и муниципальном управлении.

Внесены следующие изменения и дополнения:

Протокол от 14.05.2020 № 10  
Зав. кафедрой А. Ю. Юдинцев, доцент

---

# 1. Перечень компетенций, с указанием этапов их формирования в процессе освоения образовательной программы

Компетенции	Показатели	Наименование оценочного средства
<b>Начальный этап формирования компетенций</b> осуществляется в период освоения учебной дисциплины и характеризуется освоением учебного материала		
ОПК-1: готовностью применять методы математики, физики, химии, системного анализа, теории управления, теории знаний, теории и технологии программирования, а также методов гуманитарных, экономических и социальных наук	<p>Знает:</p> <ul style="list-style-type: none"> <li>о законодательном, административном, организационном, программно-техническом уровнях информационной безопасности.</li> </ul> <p>Умеет:</p> <ul style="list-style-type: none"> <li>правильно выбирать меры законодательного, административного, организационного и программно-технического уровня для обеспечения информационной безопасности.</li> </ul> <p>Владеет:</p> <ul style="list-style-type: none"> <li>навыками поиска необходимой информации в законах и нормативных документах для реализации мер информационной безопасности.</li> </ul>	Практические задания к лабораторным работам. Тест.
ПК-1: способностью принимать научно-обоснованные решения на основе математики, физики, химии, информатики, экологии, методов системного анализа и теории управления, теории знаний, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	<p>Знает:</p> <ul style="list-style-type: none"> <li>виды сервисов информационной безопасности программно-технического уровня.</li> </ul> <p>Умеет:</p> <ul style="list-style-type: none"> <li>работать с утилитами ядра Linux в GUI и CLI.</li> </ul> <p>Владеет:</p> <ul style="list-style-type: none"> <li>навыками выбора типовых средств защиты информации.</li> </ul>	Практические задания к лабораторным работам. Тест.
<b>Базовый этап формирования компетенций</b> (формируется по окончании изучения дисциплины)		

<p>ОПК-1: готовностью применять методы математики, физики, химии, системного анализа, теории управления, теории знаний, теории и технологии про- граммирования, а также методов гуманитарных, экономических и социальных наук</p>	<p>Знает:</p> <ul style="list-style-type: none"> <li>• основные законы и нормативные документы в сфере информационной безопасности, меры административного и организационного уровня информационной безопасности;</li> <li>• сервисы информационной безопасности программно-технического уровня.</li> </ul> <p>Умеет:</p> <ul style="list-style-type: none"> <li>• применять законы и нормативные документы, меры административного и организационного уровня информационной безопасности для организации комплексной системы защиты информации;</li> <li>• использовать сервисы информационной безопасности программно-технического уровня для проектирования, разработки и эксплуатации информационных систем.</li> </ul> <p>Владеет:</p> <ul style="list-style-type: none"> <li>• методиками разработки документации административного и организационного уровня информационной безопасности для организации комплексной системы защиты информации;</li> <li>• навыками внедрения и эксплуатации сервисов информационной безопасности программно-технического уровня.</li> </ul>	<p>Практические задания к лабораторным работам. Тест.</p>
<p>ПК-1: способностью принимать научно- обоснованные решения на основе математики, физики, химии, информатики, экологии, методов системного анализа и теории управления, теории знаний, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности</p>	<p>Знает:</p> <ul style="list-style-type: none"> <li>• концепции построения сетевой инфраструктуры предприятия;</li> <li>• сервисы информационной безопасности программно-технического уровня.</li> </ul> <p>Умеет:</p> <ul style="list-style-type: none"> <li>• устанавливать и настраивать сервисы информационных систем в соответствии с требуемым уровнем безопасности;</li> <li>• использовать сервисы информационной безопасности программно-технического уровня.</li> </ul> <p>Владеет:</p> <ul style="list-style-type: none"> <li>• навыками настройки и администрирования типовых средств защиты информации;</li> <li>• навыками внедрения и эксплуатации сервисов информационной безопасности программно-технического уровня.</li> </ul>	<p>Практические задания к лабораторным работам. Тест.</p>
<p><b>Заключительный этап формирования компетенций</b> направлен на закрепление определенных компетенций в период прохождения практик, НИР, ГИА</p>		

## 2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Показатели выявляются путём соотнесения критериев: когнитивный (знания), инструментальный (умения, навыки), праксеологический (опыт), с этапами процесса формирования компетенций, охарактеризованными выше.

Поскольку для промежуточного контроля используется такая форма контроля, как экзамен, по итоговому баллу (в 100-балльной шкале) ставится отметка, в соответствии с табл. 2.

Таблица 2.

Сопоставление шкал оценивания

100-балльная шкала	0–49	50–69	70–89	90–100
Бинарная шкала	Не зачтено	Зачтено		

Для оценивания выполнения практических заданий применяются следующие показатели:

1. полнота выполнения задания;
2. своевременность выполнения задания;
3. логическая последовательность и рациональность выполнения задания;
4. уровень самостоятельности выполнения задания;
5. уровень творчества и новаторства при выполнении задания.

В соответствии с этими показателями, на основе табл. 3 выставляется оценка за каждое выполненное задание.

При выполнении тестирования обеспечивается самостоятельность выполнения тестов: из аудитории удаляются посторонние, преподавателем контролируется неиспользование слушателем интернет-источников, учебников и иных пособий, за исключением личного конспекта слушателя (допускается, как рукописный, так и электронный вариант). Тестирование проводится в ЭУМК на базе образовательного портала АлтГУ, за ограниченное время. Оценка выставляется автоматически (по окончании теста или отведённого времени). Эта оценка отражает, в процентном отношении, долю правильных ответов на тестовые вопросы. Для перевода этой оценки в другие шкалы можно использовать табл. 2 или 3. Для подготовки к тестированию студенты используют контрольные вопросы.

Для оценивания ответа на экзамене применяются следующие показатели:

1. полнота изложения теоретического материала;
2. полнота и правильность решения практического задания;
3. правильность и/или аргументированность изложения (последовательность действий);
4. самостоятельность ответа;
5. культура речи.

В соответствии с этими показателями, на основе табл. 4 оценивается ответ на экзаменационные вопросы.

Оценивание выполнения практических заданий

4-балльная шкала (уровень освоения)	100-балльная шкала	Критерии
Отлично (повышенный уровень)	90–100	Студентом задание выполнено самостоятельно и в срок. При этом составлен правильный алгоритм выполнения задания, в логических рассуждениях, в выборе ПО и методах его применения нет ошибок, получен верный ответ, задание выполнено рациональным способом.
Хорошо (базовый уровень)	70–89	Студентом задание выполнено с небольшими подсказками преподавателя, возможно, с небольшой задержкой сроков. При этом составлен правильный алгоритм выполнения задания, в логическом рассуждении и решении нет существенных ошибок; правильно сделан выбор ПО и методов его применения для выполнения задания; есть объяснение выполнения, но задание выполнено не рациональным способом или допущено не более двух несущественных ошибок, получен верный ответ.
Удовлетворительно (пороговый уровень)	50–69	Студентом задание выполнено с подсказками преподавателя, с большой задержкой сроков. При этом задание понято правильно, в логическом рассуждении нет существенных ошибок, но, возможно, допущены существенные ошибки в выборе ПО и методов его применения или в составлении документации; задание выполнено не полностью или в общем виде.
Неудовлетворительно (уровень не сформирован)	0–49	Студентом задание не выполнено.

### 3. Типовые контрольные задания или иные материалы, необходимые для оценки планируемых результатов обучения по дисциплине, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

#### 3.1. Примерные темы лабораторных работ, практических, индивидуальных заданий

##### Лабораторная работа №1

##### Создание безопасной экспериментальной среды

Для создания безопасной экспериментальной среды можно использовать выделенные компьютеры (не включённые в корпоративную сеть), однако более удобным решением, в современных условиях, является создание такой среды на основе виртуализации. Сейчас даже на рабочих станциях можно запустить несколько виртуальных машин.

Для создания полноценной среды необходимо развернуть *сетевую ОС с серверными службами*. Поэтому необходимо создать виртуальную машину с ОС семейства GNU/Linux. В данных условиях Вы можете установить ОС Ubuntu ([репозиторий](#) поддерживается управлением информатизации АлтГУ) или ОС Rosa (репозиторий поддерживается кафедрой ПИЭГМУ МИЭМИС АлтГУ).

##### Задание 1. Создание виртуальной машины

Используя VirtualBox создайте и настройте новую виртуальную машину.

1. Работая в компьютерном классе, проверьте, имеется ли в директории D:\ISO<sup>1</sup> образ диска с дистрибутивом ОС, посмотрите, как называется эта операционная система. Скопируйте в директорию D:\ISO образ диска с дистрибутивом ОС (файл ROSA.FRESH.KDE4.R11.x86\_64.uefi.iso) с ресурса <ftp://10.0.12.224/>. Если на ПК имеется скачанный дистрибутив предыдущей версии, можно использовать его. При наличии

<sup>1</sup>Если отсутствует диск D:, используйте каталог C:\VirtualBox.

## Оценивание ответа на экзамене

4-балльная шкала (уровень освоения)	Критерии
Отлично (повышенный уровень)	Студентом дан полный, в логической последовательности развернутый ответ на поставленный вопрос, где он продемонстрировал знания предмета в полном объеме учебной программы, достаточно глубоко осмысливает дисциплину, самостоятельно, и исчерпывающе отвечает на дополнительные вопросы, приводит собственные примеры по проблематике поставленного вопроса, решил предложенные практические задания без ошибок.
Хорошо (базовый уровень)	Студентом дан развернутый ответ на поставленный вопрос, где студент демонстрирует знания, приобретенные на лекционных и семинарских занятиях, а также полученные посредством изучения обязательных учебных материалов по курсу, дает аргументированные ответы, приводит примеры, в ответе присутствует свободное владение монологической речью, логичность и последовательность ответа. Однако допускается неточность в ответе. Решил предложенные практические задания с небольшими неточностями.
Удовлетворительно (пороговый уровень)	Студентом дан ответ, свидетельствующий в основном о знании процессов изучаемой дисциплины, отличающийся недостаточной глубиной и полнотой раскрытия темы, знанием основных вопросов теории, слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры, недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа и решении практических заданий.
Неудовлетворительно (уровень не сформирован)	Студентом дан ответ, который содержит ряд серьезных неточностей, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы, незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов, неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Выводы поверхностны. Решение практических заданий не выполнено. Т.е студент не способен ответить на вопросы даже при дополнительных наводящих вопросах преподавателя.

опыта работы в GNU/Linux Вы можете использовать дистрибутив **Ubuntu**, **Debian** или **Linuxmint** (для этих ОС поддерживаются репозитории в АлтГУ)

- Запустите VirtualBox, посмотрите настройки (▷ Файл ► Свойства), обратите внимание на *Хост-клавишу*. Посмотрите, куда сохраняются виртуальные машины. Если работаете в компьютерном классе, то задайте папку для машин D:\.
- Создайте новый образ виртуальной машины для *Вашей* ОС, например:

**Имя** — ROSA-2021-фамилия;

**Операционная система** — Linux;

**Версия** — Mandriva 64.

Внимательно прочитайте рекомендации мастера, используйте свойства по умолчанию, предлагаемые мастером, кроме двух:

**тип жёсткого диска** — Virtual Machine Disk (VMDK);

**размер** — 20 ГБ.

- Посмотрите *свойства* полученного образа. Увеличьте размер *основной памяти* до 1024 МБ (можно больше, но не более половины от доступной памяти). Если есть возможность, увеличьте число процессоров до 1/2 от доступного количества. Размер *видеопамяти* увеличьте (тоже до 1/2 от доступной).

5. Уберите из загрузочных устройств FDD («дискета») и свяжите с приводом оптических дисков скачанный ISO-образ с дистрибутивом (расположенным в D:\ISO). Если на компьютере есть аудиокарта, то выберите на вкладке **Аудио** **Аудиоконтроллер Intel HD Audio**.
6. Посмотрите «сетевые адаптеры», выберите тип подключения **Сетевой мост**. Добавьте ещё один сетевой адаптер, выберите для него тип подключения NAT.

### Задание 2. Установка ОС

1. Запустите созданную виртуальную машину. По нажатию F12 можно изменить источник загрузки.
2. Следуя руководству мастера, установите гостевую ОС. Для управления устройствами виртуальной машины можно использовать меню или пиктограммы внизу окна.  
Будьте внимательны, **пароль Администратора (root), задаваемый в конце установки ОС подлежит надёжному хранению**, т. к. в случае утери восстановлению/изменению не подлежит. Потребуется переустановка ОС!
3. Зайдите в гостевую ОС и посмотрите установленные компоненты.

### Задание 3. Работа с виртуальной машиной и гостевой ОС GNU/Linux

1. Установите общий буфер обмена в режим двунаправленный (на вкладке **Дополнительно** в **Общих** > свойствах виртуальной машины).
2. Проверьте работу сети гостевой ОС, при необходимости измените настройки виртуальной сетевой карты.
3. Посмотрите возможности настройки ОС (через пиктограмму в панели быстрого запуска).
4. Добавьте пользователя **user** с паролем **user** (отдельную группу создавать не надо).
5. Внимание, этот пункт выполняется только в локальной сети АлтГУ!

Для ОС **Rosa**, запустите **менеджер источников программ**, отключите все включенные источники и добавьте (через меню ► **Файл**) *пользовательский источник* (для Rosa):

- тип — Сервер HTTP;
- URL — <http://10.0.12.224/rosa/>;
- включите все переключатели.

После добавления этого репозитория появится сообщение об ошибке, связанной с невозможностью добавить 32-разрядный репозиторий (ничего страшного, этого репозитория действительно нет).

6. Внимание, этот пункт выполняется только в локальной сети АлтГУ!  
Для других ОС (Ubuntu, Debian, Linuxmint), следуйте указаниям, приведённым на <http://linuxupdate.asu.ru/>.
7. Выполните обновление системы.
8. Установите систему управления проектами Planner, редактор BlueFish и ещё какой-нибудь софт по желанию (например, игру).
9. Посмотрите оборудование виртуальной машины.
10. Посмотрите в VirtualBox, как работает Ваша машина. Сделайте *снимок* машины.
11. Измените настройки рабочего стола, окон. Можете даже «сломать» машину.
12. Выключите машину (можно аварийным способом). Восстановите состояние машины из снимка.



13. Создайте и подключите «общую папку». Для подключения используйте (из-под root) `mount -tvboxsf папка точкаМонтирования`, где **папка** — название общей папки в VirtualBox, а **точкаМонтирования** может быть любой доступной директорией в гостевой ОС, например в Вашей домашней директории или `/mnt`.

Для работы с общими папками на Linux необходимо внести пользователя гостевой системы в группу `vboxsf`. Для подключения в виртуальной машине портов USB необходимо добавить пользователя хост-системы в группу `vboxusers`. Для включения режима USB 2.0 и USB 3.0 необходимо установить VirtualBox Extension Pack с сайта <https://www.virtualbox.org/>.

#### Задание 4. Пользовательские настройки OSGNU/Linux

1. Познакомьтесь с интерфейсом.
2. Изучите пиктограммы быстрого запуска и пиктограммы запущенных программ (в трее).
3. Посмотрите оборудование компьютера.
4. Настройте раскладку клавиатуры (включите флаг страны).
5. Добавьте в панель быстрого запуска виджет «Классическое меню запуска приложений».
6. Измените настройки рабочего стола, окон. Увеличьте число рабочих столов до 4–6.
7. Посмотрите и настройте графические эффекты рабочего стола.

#### Задание 5. Работа с файлами в GNU/Linux

1. Используя Dolphin (также доступен из панели быстрого запуска), посмотрите имеющиеся ресурсы, сделайте вид «две панели» (`F3`).
2. Перейдите в домашнюю директорию, посмотрите скрытые файлы (`Alt+.`), воспользуйтесь фильтром (`Ctrl+I`).
3. Включите терминал в Dolphin (`F4`), посмотрите процессы (`ps`), посмотрите справку по этой команде (`ps --help`).
4. Можно выполнить и сохранить необходимые настройки Dolphin через меню **Настройка ► Настроить Dolphin**.
5. Узнайте (в Windows) полное название сетевых дисков (`P:`, `U:`) и подключите эти ресурсы, используя Dolphin. Для удобства можно добавить часто используемые ресурсы в «точки входа».
6. Попробуйте скопировать *окно*, вставить изображение в документ, сохранить этот документ в формате PDF.
7. Создайте в другой папке ссылку на этот документ. Откройте файл-ссылку, измените, сохраните и закройте. Откройте оригинальный файл, посмотрите изменения.
8. Запустите консоль. Определите своё местонахождение в файловой системе (`pwd`). Посмотрите список файлов (`ls`). Посмотрите подсказку по команде (например, `ls --help`). Посмотрите документацию (`manual`) по команде. (например, `man ls`).
9. Запустите консольный файловый менеджер Midnight Commander (`mc`). Изучите доступные команды.

#### Задание 6. Работа группы виртуальных машин

1. Узнайте у одноклассников адреса их виртуальных машин.
2. Установите сетевое взаимодействие с другими виртуальными машинами в классе. Для этого можно предоставить общий доступ к некоторой папке на своей машине и зайти на такой же ресурс, предоставленной на другой машине.
3. Зайдите на чужую машину под логином `user`.
4. Попробуйте зайти на чужую машину под суперпользователем.
5. Попробуйте выключить чужую машину.
6. Выключите свою виртуальную машину.

## Лабораторная работа №2

### Корпоративная сеть

Перед началом выполнения работы запустите браузер (откройте какой-нибудь сайт), установите сетевые соединения по другим протоколам (`smb`, `ssh`, `ftp`, `webdav`, ...).

#### Задание 1. Сетевые настройки

Используя интерфейс ОС или системные сетевые утилиты (`ipconfig`, `ifconfig`), узнайте и поместите в отчёт сетевые настройки Вашего *хост-компьютера* (с ОС Windows) и *виртуальной машины* (гостевой ОС GNU/Linux):

1. Имя компьютера.
2. Маску сети.
3. IP-адрес, номер сети и номер узла.
4. Какой используется адрес: статический или динамический?
5. MAC-адрес.
6. Какая сетевая карта используется (производитель, чипсет)?
7. Сетевой шлюз.

В Linux (кроме графических инструментов рабочего стола) можно получить подробные сведения с помощью утилиты `lshw`, например:

```
lshw -class network
```

А вся информация о сетевых соединениях записана в текстовых файлах в папке `/etc/sysconfig/network-scripts`.

#### Задание 2. Работа в сети

Используя системные сетевые утилиты, узнайте и поместите в отчёт следующую информацию:

1. *Среднее время* обмена пакетами с узлом `public.edu.asu.ru` и `www.securitylab.ru` (`ping`).
2. Маршрут к произвольному доступному удалённому узлу в глобальной сети Интернет (например, `public.edu.asu.ru`, `82.179.31.34`) (`tracert`).
3. В ОС Windows с помощью утилиты `net` посмотрите список сетевых подключений.  
Подключите любой общий сетевой ресурс как диск Y:. Снова посмотрите список сетевых подключений и добавьте его в отчёт.
4. Для более наглядного выполнения последующих заданий, установите несколько сетевых соединений (например, открыв страницы в браузере, открыв сетевые ресурсы в Dolphin).

С помощью утилиты `netstat` посмотрите:

- 4.1. Активные подключения (имя, локальный и внешний адреса, состояние), если имеются (`netstat`).
- 4.2. Статистику Ethernet (`netstat -s`).
- 4.3. Таблицу маршрутов (`netstat -r`).
- 4.4. Вывести список всех открытых TCP-портов (`netstat -at` или `netstat -ant` (`n` — без преобразования имён, так быстрее)). По какому количеству портов Ваша машина слушает сеть? Сколько соединений установлено?
- 4.5. Какие процессы связаны с конкретными портами? (`netstat -anp`)

#### Задание 3. Слушаем сеть

1. С помощью сетевого браузера EtherApe посмотрите свою локальную сеть. Просмотрите работающие узлы и протоколы, наблюдайте за активностью сети. Сделайте скриншот окна браузера.

2. С помощью утилиты **netstat** посмотрите информацию о сетевых интерфейсах TCP в реальном времени (**netstat -ic**).
3. С помощью утилиты **lsof** посмотрите все открытые объекты и процессы, открывшие их.
4. С помощью утилиты **lsof** посмотрите все открытые порты и процессы, открывшие их (**lsof -i**).
5. С помощью утилиты **tcpdump** посмотрите:
  - 5.1. Информацию о всех перехваченных сетевых пакетах.
  - 5.2. Информацию о всех перехваченных сетевых пакетах по сетевым интерфейсам, связанным с первым и вторым сетевым адаптером (**tcpdump -i<интерфейс>**).
  - 5.3. Информацию о всех сетевых пакетах определённого узла (например, **proxy.asu.ru**) в сети (**tcpdump -i<интерфейс> -vvvv host <адрес>**). Рассмотрите варианты различной детализации информации (ключ **v**).
  - 5.4. Информацию о всех сетевых пакетах обмена между определёнными двумя (соседними) узлами в сети (**tcpdump -i<интерфейс> -vvvv host <адрес1> and <адрес2>**).

#### Задание 4. Сканирование чужой сети

<https://hackertarget.com/nmap-online-port-scanner/>

Используйте для сканирования утилиту **nmap** (можно в командной строке, можно через графический интерфейс, например **zenmap**, **nmapsi4**). Изучите работу с **nmap**. Просканируйте сетевые узлы **10.0.12.15**, **10.0.12.224**, **82.179.31.34**, **scanme.nmap.org** и **demo.testfire.net**.

По результатам сканирования узнайте:

1. операционную систему хостов;
2. псевдонимы хостов (если есть);
3. IP-адрес хостов;
4. открытые порты хостов;
5. количество закрытых портов;
6. какое ПО используется хостом (использует доступные порты);
7. маршрут к хосту;
8. состояние хостов (включен или выключен).

Можно для отчёта сделать скриншоты.

#### Дополнительно:

**Snort** — свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом, способная выполнять регистрацию пакетов и в реальном времени осуществлять анализ трафика в IP-сетях.

**Shodan** — это первая (и, пожалуй, ведущая) поисковая система по Интернету вещей, существующая с 2009 года. **Shodan** назвали в честь главного злодея (точнее, злодейки) в серии компьютерных игр **System Shock** — в игре это был крайне злобный искусственный интеллект. Конечно, эта поисковая система не настолько безжалостна, как ее прототип, но и она способна причинить немало вреда.

Сохраните отчёт в файл и выложите его на Moodle. **Лабораторная работа №3**

#### Первые шаги к безопасной ОС

В этой работе требуется выполнить настройки в операционной системе, которые позволят повысить безопасность и производительность рабочей станции.

#### Задание 1. Управление службами

Используя графические инструменты или непосредственно редактируя файлы настроек, выполните следующие действия:

1. Просмотрите запущенные службы (если непонятно, что за служба, посмотрите информацию о ней).
2. Ненужные службы потребляют ресурсы и создают дополнительные уязвимости в системе безопасности. Отключите ненужные службы (по крайней мере очевидные), обратите внимание на CUPS.
3. Включите (если ещё не включен) SSH-сервер.

4. Установите интерпретатор PHP (для Apache), phpMyAdmin, веб-сервер Apache, СУБД MariaDB, антивирус clamav. Запустите и проверьте установленные продукты.

Службы в UNIX/Linux системах запускаются с правами **root**. Войдя под **root** для запуска службы (демона) **apache** нужно набрать в командной строке следующую команду:  
**service httpd start**

Аналогично запускаются и другие службы (буква **d** в конце имени указывает на то, что это служба, «демон»).

Проверить Apache можно в браузере, набрав адрес своей машины (на своей машине можно ввести **localhost** или **127.0.0.1**).

5. Установите «запуск служб при включении» для Apache (**httpd**) и MariaDB (**mysqld**) через GUI или **chkconfig** (текстовый интерфейс для **/etc/rc[0-6].d**).
6. Просмотрите запущенные службы с помощью утилиты **systemctl**, установленные службы с помощью **systemctl list-unit-files**. Запущена ли служба **ssh**? Если не запущена, то запустите.

Запустить службу из консоли можно и через утилиту **systemctl** с командой **start** и названием службы, например: **systemctl start sshd**.

Посмотрите открытые порты (**systemctl list-sockets**). Чтобы увидеть не только активные соединения, воспользуйтесь командой **systemctl list-sockets -all**.

Добавьте в отчёт список запущенных служб и список открытых портов (вместе с командами).

## Задание 2. Изменение заданных по умолчанию настроек

Используя графические инструменты или непосредственно редактируя файлы настроек, выполните следующие действия:

1. Посмотрите в настройках список зарегистрированных пользователей. Посмотрите *информацию об учётной записи* пользователя (свой логин). Посмотрите *информацию о пароле* пользователя, включите срок действия пароля **365 дней**, предупреждать об изменении за **неделю**. Если есть пользователь «Гость» (**guest**), заблокируйте его учётную запись.

Список пользователей, которые в текущий момент зарегистрированы в системе активных пользователей можно вывести командой **who**.

Посмотрите *свойства* своей *Домашней папки*. Измените *права* (просмотр, изменение, доступ) на эту папку, в соответствии с Вашими потребностями.

Подтвердите работу скриншотами.

2. Все СУБД рекомендуется сначала проверять из консоли. Консоль для MariaDB называется **mysql** (так же, как и для СУБД MySQL). Запустите консоль MariaDB (из под **root**).

Найдите в Интернете пароли по умолчанию для MariaDB (MySQL) и др. сервисов. Добавьте этот список и адрес в отчёт.

Попробуйте зайти в СУБД через графический интерфейс (**http://localhost/phpmyadmin**). Сделайте скриншот результата.

Попробуйте зайти на чужой компьютер, как **user**, и запустить консоль **mysql**.

3. Исправьте обнаруженный недостаток. Для MariaDB (MySQL) изменить пароль можно следующей командой:

```
mysqladmin -u пользователь password новый_пароль
```

После изменения пароля войти через консоль можно только с ключом **-p**:

```
mysql -p [-u пользователь]
```

Ещё раз проверьте работу веб-сервера и СУБД (через веб-интерфейс). Сделайте скриншот результата.

Добавьте в отчёт содержимое окна консоли (терминала).

### Задание 3. Защита ОС

1. Откройте «параметры входа в систему», посмотрите текущие настройки. Посмотрите, кому разрешено *выключать и перезагружать компьютер*.

Запретите вход в систему и работу в обычном режиме для пользователя `root`.

Не допускайте *автоматический вход* в систему и вход без пароля.

Подтвердите работу скриншотами.

2. Включите *файервол*. Разрешите доступ только к тем службам, которые у Вас используются. Проверьте открытые порты (см. предыдущую работу). Проверьте доступность сервисов с хоста (из основной ОС) или с другой машины.

Подтвердите работу скриншотами.

3. Выполните *настройку аутентификации* для системных утилит. Не допускайте к настройкам сети и системы никого, кроме `root`.

Подтвердите работу скриншотами.

4. Настройте антивирусный сканер (используйте графический интерфейс clamtk). Задайте автоматическое обновление вирусной базы и ежедневное сканирование домашней папки.

Подтвердите работу скриншотами.

### Задание 4. Резервное копирование

1. Создайте новый виртуальный диск размером 200 МБ с названием `backups` и подключите к своей виртуальной машине.

2. Используя утилиту для работы с дисками (например, `drakdisk`), задайте для `backups` файловую систему `ext4`, отформатируйте его и примонтируйте в `/mnt/.backups`.

3. Используя доступный инструмент, составьте «План резервного копирования»:

- тип — версионное резервное копирование;
- источники — папка `Документы`;
- место хранения — диск `backups` (`/mnt/.backups`);
- расписание — интервал 1 день;
- дополнительно — проверка целостности.

4. Выполните резервное копирование. Посмотрите файл журнала, добавьте его содержимое в отчёт.

### Лабораторная работа №4

#### Тестирование веб-сайтов

В этой работе Вы должны познакомиться с технологиями тестирования на проникновение, инструментами для проведения такого тестирования, рекомендациями по разработке надёжных веб-приложений и веб-сервисов.

## Проект OWASP

Большая часть современных приложений используют сетевые технологии и по сути являются или веб-приложениями (динамические сайты) или веб-сервисами. Для разработчиков таких приложений одним из наиболее значимых вопросов является безопасность как всей инфраструктуры (обычно обеспечивается хостинг-провайдером), так и скриптов (обеспечивается разработчиком).

Проблема осложняется тем, что для написания сайтов широко используются готовые решения в виде различных фреймворков и CMS, где уровень безопасности поставляется «из коробки», и повлиять на него очень проблематично. Стоит отметить, что каждый этап рефакторинга, добавления/изменения функционала на сайте зачастую снижает уровень безопасности. Если на этапе запуска проекта уровень защиты был протестирован и находился на допустимом уровне, то впоследствии могут появиться критические уязвимости, обнаруживающие себя слишком поздно.

Список возможных уязвимостей веб-приложений и веб-сервисов весьма обширен, так как сайты и сервисы используют очень разнообразный стек технологий, который, в свою очередь, развивается достаточно интенсивно. Ограниченная версия этого списка выглядит примерно так:

- PHP-инъекция;
- PHP-инъекция через загрузку файлов;
- SQL-инъекция;
- межсайтовый скриптинг (XSS);
- взлом сервисов аутентификации и управления сессиями;
- небезопасные прямые ссылки на объект;
- некорректная конфигурация безопасности инфраструктуры;
- доступность конфиденциальных данных;
- отсутствие контроля доступа на уровне функции;
- межсайтовая подделка запроса (CSRF);
- использование компонентов с известными уязвимостями;
- непроверенные перенаправления и переадресация;
- демонстрация ошибок пользователю;
- доступность данных о характеристиках системы пользователю;
- доступность данных о программном коде пользователю;
- возможность задания глобальных переменных;

С 2001 года существует открытый проект обеспечения безопасности веб-приложений (Open Web Application Security Project) — OWASP. Сообщество OWASP включает в себя корпорации, образовательные организации и частных лиц со всего мира, OWASP состоит примерно из 190 местных отделений, располагающихся по всему миру (Российское представительство OWASP находится здесь: <https://www.owasp.org/index.php/Russia>) и тысяч участников в листах рассылки проекта. Сообщество работает над созданием статей, учебных пособий, документации, инструментов и технологий, находящихся в свободном доступе.

OWASP не аффилирован ни с одной компанией, занимающейся разработкой технологий, он поддерживает грамотное использование технологий безопасности. Проект избегает аффилирования, так как полагает, что свобода от влияния со стороны других организаций может облегчить распространение беспристрастной, полезной и дешевой информации о безопасности приложений.

Участники сообщества OWASP делают приложения безопаснее, учитывая человеческий фактор и технологический уровень. Наиболее востребованные документы, опубликованные OWASP, включают в себя:

**Руководство OWASP —**

[www.owasp.org/index.php/OWASP\\_Guide\\_Project](https://www.owasp.org/index.php/OWASP_Guide_Project);

## Обзорное руководство по программированию —

[www.owasp.org/index.php/Category:OWASP\\_Code\\_Review\\_Project](http://www.owasp.org/index.php/Category:OWASP_Code_Review_Project);

## Руководство по тестированию OWASP —

[https://www.owasp.org/index.php/OWASP\\_Testing\\_Project](https://www.owasp.org/index.php/OWASP_Testing_Project);

## Проект Топ-10 OWASP —

[www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

Руководство по Разработке OWASP даёт практические советы и содержит примеры кода на J2EE, ASP.NET и PHP. Руководство по Разработке охватывает обширный массив вопросов безопасности для уровня приложений, таких как SQL-инъекции, фишинг, обработка кредитных карт, фиксация сессий, подделка межсайтовых запросов, согласование и конфиденциальность.

OWASP создал стандарт [OWASP Application Security Verification Standard \(ASVS\)](#). Основная цель OWASP ASVS — это стандартизация диапазона охвата и уровня строгости доступных на рынке приложений, обеспечивающих безопасность, а также создание набора коммерчески успешных открытых стандартов, приспособленных для специализированных веб-технологий. Сборник для веб-приложений уже опубликован, сборник для веб-сервисов находится в процессе разработки.

Самыми распространёнными инструментами OWASP являются:

- тренировочная среда WebGoat  
([https://www.owasp.org/index.php/Category:OWASP\\_WebGoat\\_Project](https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project));
- прокси-анализатор Zed Attack Proxy  
([https://www.owasp.org/index.php/OWASP\\_Zed\\_Attack\\_Proxy\\_Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)); .NET инструменты  
([https://www.owasp.org/index.php/Category:OWASP\\_.NET\\_Project](https://www.owasp.org/index.php/Category:OWASP_.NET_Project)).

### Задание 1. Использование IBM Security AppScan Standard для сканирования веб-приложений на наличие уязвимостей безопасности

Доступная версия IBM Security AppScan Standard позволяет сканировать только сайт `demo.testfire.net`. Для этого сайта есть доступ в один аккаунт — имя пользователя: `jsmith` пароль: `demo1234`.

Сканирование AppScan состоит из двух этапов: анализ и тестирование.

**Анализ** — сайту отправляются запросы для сбора данных о нем и его структуре в автоматическом режиме или вручную. AppScan анализирует ответы, выполняет поиск потенциальных уязвимостей и создает тестовые запросы.

**Тестирование** — AppScan отправляет тысячи пользовательских тестовых запросов. Он записывает и анализирует ответы приложения, обнаруживая неполадки защиты, определяя уровень риска и предлагая рекомендации.

В ходе полностью автоматического сканирования после завершения первой фазы анализа и тестирования AppScan переходит к новой фазе для обработки информации, полученной в ходе тестирования. Сканирование завершается после выполнения настроенного числа фаз сканирования.

Анализ веб-приложения или веб-службы перед проверкой с помощью AppScan можно выполнить тремя способами:

- С помощью AppScan: продукту AppScan передаются начальный URL и идентификационные данные для автоматического анализа. Кроме того, можно вручную проверить сайт, чтобы предоставить AppScan доступ к областям, для обращения к которым требуются специальные действия пользователя.
- С помощью внешнего устройства для анализа веб-служб RESTful или других веб-служб, отличных от SOAP или служб SOAP, не требующих конвертов защиты — запросы отправляются на сайт с помощью мобильного телефона, симулятора или эмулятора; AppScan настраивается как записывающий прокси-сервер.
- С помощью GSC (Generic Service Client, общий клиент служб): при наличии файла WSDL интегрированный клиент (GSC) может создать интерфейс, в котором отображаются службы и можно ввести параметры и просмотреть результаты.

Результаты сканирования удобно представить в виде отчёта. В AppScan можно управлять содержимым и макетом отчётов, доступны отчёты различных типов:

**Отчёт о защите** — перечислены обнаруженные уязвимости защиты.

**Промышленный стандарт** — указывает, соответствует ли приложение требованиям выбранных стандартов (PCI, OWASP Top 10, SANS или WASC).

**Соблюдение требований законодательства** — указывает, соответствует ли приложение требованиям законодательства (например, HIPAA, GLBA, SOX, California SB 1386 и AB 1950).


**Разностный анализ** — сравнивает два набора результатов сканирования и отображает различия URL и/или неполадок защиты.

**Шаблоны отчётов** — позволяет создать отчёты с пользовательскими данными и параметрами форматирования в виде файлов MS Word (.doc).


1. Зайдите на сайт `demo.testfire.net`. Посмотрите разделы сайта. Попробуйте зайти в аккаунт `jsmith` (пароль: `demo1234`). Посмотрите доступные для этого пользователя ресурсы.
2. Запустите IBM Security AppScan Standard. Закройте окно приветствия.
3. Создайте новое сканирование (▷ Файл ▷ Создать...).
4. Выберите шаблон регулярного сканирования (Regular Scan).
5. В мастере настройки сканирования выберите метод анализа AppScan.
6. Настройте сканирование с помощью AppScan:
  - прокси: из настроек браузера;
  - начальный URL сканирования: `demo.testfire.net`.
7. Выберите из шаблонов стратегию тестирования — Полный. На странице Login Method задайте метод входа на сайт Автоматический и задайте параметры авторизации для входа на сайт:
  - логин: `jsmith`;
  - пароль: `demo1234`;

Задайте файл для сохранения результатов сканирования.

8. Запустите сканирование. Сначала будет выполнено оценочное сканирование, после анализа его результатов будут выданы рекомендации по изменению параметров для оптимизации стратегии сканирования веб-сайта.
9. Выполните выданные рекомендации (измените параметры, настройки сканирования). Некоторые параметры среды исполнения веб-приложения можно выяснить изучая сайт, используя обычный браузер.

Полный доступ к параметрам **конфигурации сканирования** можно получить через соответствующую пиктограмму или меню ▷ Сканирование ► Конфигурация сканирования (.

Чем точнее Вы укажете известные данные, тем быстрее будет произведено тестирование и анализ сайта.

10. Просмотрите в разделе ТЕСТ выбранные Стратегии тестирования (кнопкой  раскрываются группы). Здесь можно узнать о сути тестируемой уязвимости (на вкладке Сообщение) и Рекомендации по исправлению этой уязвимости.
11. Примените рекомендации (помеченные). При этом запустится повторное сканирование, более глубокое, для полного экспертного анализа.

В процессе тестирования возможны обнаружения уязвимостей, они будут скапливаться в разделе Неполадки (▷ Вид ► Защита). По умолчанию список Упорядочен по приоритету, По убыванию.

Во время сканирования можно просмотреть найденные уязвимости (Информация о неполадке), их описание Сообщение) и рекомендации для их устранения (Рекомендации по исправлению).

Во вкладке Запрос/Ответ можно просматривать описание теста, посылаемый запрос (начинается с GET) и ответ сервера (начинается с HTTP). Здесь можно выполнять поиск текста, открывать запрос в браузере. Через локальное меню ▷ Опции можно задать параметры выбранному тесту.



12. В разделе Данные (▷ Вид ► Данные приложения) можно просмотреть сгенерированные для тестирования данные (параметры, запросы, и т. д.). Обратите особое внимание на вкладку Требуется взаимодействие с пользователем, если в этом разделе есть данные, необходимо вручную ввести необходимые значения.
13. В разделе Задачи (▷ Вид ► Задачи исправления) можно посмотреть выданные рекомендации для устранения обнаруженных уязвимостей. В крайнем левом столбце представлена в виде дерева файловой системы логического каталога сайта (На основе URL) или связанного списка файлов физического каталога сайта (На основе содержимого). Выбирая ветки этого дерева можно видеть отфильтрованные рекомендации для выбранной ветки (папки или файла).
14. После окончания сканирования, просмотрите Протокол сканирования (▷ Вид ► Протокол сканирования).
15. Откройте в разделе XSS первый тест (amCreditOffer (Cookie)), прочитайте о нём информацию, просмотрите запрос этого теста в браузере, пометьте этот тест, как не имеющий уязвимостей.
16. Откройте мастер создания отчётов, добавьте в Макет верхний колонтитул со своей фамилией, инициалами и номером группы. Создайте 3 отчёта:
  - Защита — используйте шаблон Подробный отчёт, добавьте в содержание отчёта Запрос/Ответ.
  - Соответствие промышленным стандартам — *OWASP Top 10 2013*.
  - Соблюдение требований законодательства — выберите *Payment Application Data Security Standart*.

## Задание 2. Установка веб-приложения для тестирования

Это задание выполняется по вариантам (вариант назначается по списку группы, уточните свой вариант у преподавателя).

Требуется установить систему управления контентом (CMS) или другую систему управления службами с веб-интерфейсом, согласно своему варианту: 2

1. WordPress;
2. Joomla!;
3. WebMake;
4. ClearSilver;
5. Drupal;
6. Shop-Script;
7. MODX;
8. OpenCart;
9. PrestaShop;
10. TYPO3;
11. CMS Made Simple (CMSMS);
12. DotClear;
13. DotProject;
14. web2project;
15. phpMyAdmin;
16. phpPgAdmin;
17. RoundCubeMail;

18. UserMin-WebMail;
19. Kolab Groupware;
20. Moodle.

### Задание 3. Проведение тестирования

1. Скачайте виртуальную машину с *Kali Linux* с <ftp://10.0.12.224/>. Запустите Kali. Пароль: `admin@Kali`.
2. Запустите свою виртуальную машину с установленным веб-приложением. Узнайте IP-адрес ресурса, проверьте его доступность и работоспособность.
3. Добавьте в Sparta IP-адрес тестируемого ресурса. Выполните тестирование.
4. Укажите в отчёте, какие службы и по каким портам доступны. Подкрепите ответ скриншотом служб.
5. Добавьте в отчёт протоколы работы используемых внешних инструментов.
6. Скачайте (в Kali) «Словари для брута», например с ресурса <ftp://10.0.12.224/> (можете найти в Сети и другие словари).

Выполните подбор идентификационных данных для тех сервисов, для которых требуется аутентификация (отправьте их в Brute). Для этого могут пригодиться словари (загрузите их в Sparta в соответствующие разделы).

Добавьте в отчёт протоколы взлома (Brute).

### Лабораторная работа №5

#### Укрепление безопасности с помощью шифрования

В этой работе Вы должны познакомиться с наиболее распространёнными и доступными средствами криптографической защиты.

#### Задание 1. Знакомство с хешированием

1. Скачайте файл `AppScan_Setup.exe` с <ftp://10.0.12.224/>. Посмотрите информацию об утилитах `md5sum`, `shasum` и `shasum`.
2. Чему равна хеш-сумма файла `AppScan_Setup.exe`, посчитанная по алгоритму MD5?
3. Чему равна хеш-сумма файла `AppScan_Setup.exe`, посчитанная по алгоритму SHA-1?
4. Чему равна хеш-сумма файла `AppScan_Setup.exe`, посчитанная по алгоритму SHA-256?
5. Чему равна хеш-сумма фразы (панграммы) «Широкая электрификация южных губерний даст мощный толчок подъёму сельского хозяйства.» (в кодировке UTF-8), посчитанная по алгоритму SHA-512?

Насколько сильно изменится хеш-сумма, если вместо буквы 'ё' написать 'е'?

#### Задание 2. Настройка авторизации средствами веб-сервера Apache

После установки Apache создаётся каталог `/var/www`. Корень сайта (по умолчанию) — каталог `html`, расположенный в нём.

1. В корне своего сайта создайте каталог `private`, а в нём создайте `index.html`. В файле `index.html` напишите, что этот ресурс принадлежит «синим»/«красным» (в зависимости от Вашей принадлежности к команде). Можете, для выразительности, использовать графическое оформление страницы.
2. Установите дополнительные пакеты Apache: `auth_basic`, `auth_digest`, `authn_core`, `authn_file`, `authz_core`, `authz_groupfile`, `authz_owner`, `authz_user`.

3. В этом каталоге создайте файл `.htaccess`. Укажите в нём кодировку исходного текста индексного файла. Поэкспериментируйте с различными кодировками (при этом в браузере кодировка страниц должна быть выставлена в автоматическое определение).

Если изменения не наблюдаются, проверьте главный файл настроек — `httpd.conf` в каталоге `/etc/httpd/conf` (все локальные изменения параметров Apache должны быть разрешены).

4. Защитите каталог `private`.

- Создайте пароли для всех пользователей Вашей команды. Файл с паролями разместите в каталоге выше корневого на один уровень.
- Для аутентификации используйте хеширование MD5.
- Создайте две группы — *red* и *blue*. Организуйте доступ для себя, проверьте. Организуйте доступ для своей группы, проверьте.

5. Поместите в отчёт URL своего веб-ресурса, логин и пароль (любой допустимый) для входа на него.

### Задание 3. Обмен информацией с GnuPG

Используя GnuPG, создайте необходимые ключи и проверьте их в работе.

1. Проверьте, установлен ли у Вас GnuPG. Для этого наберите в командной строке

```
gpg2 -h
```

Если GnuPG отсутствует в системе, то установите его. Можно установить графический интерфейс управления ключами — Kpgp.

2. Попробуйте *симметричное шифрование* (на каком-нибудь файле с данными):

```
gpg2 -с файл
```

Должен появиться файл с таким же именем и с суффиксом `.gpg`. Теперь его смело можно переносить в другое место (хоть на край света). Расшифровать файл можно командой

```
gpg2 --decrypt-files файл.gpg
```

3. Сгенерируйте (с помощью мастера) пару ключей (секретный и публичный) для *асимметричного шифрования*:

```
gpg2 --gen-key
```

После заполнения данных с помощью мастера, следует задать фразу-пароль. В качестве фразы-пароля, можно указывать достаточно длинные значения, многословные.

На генерацию ключей требуется ощутимое время, в течение которого надо проявлять активность (см. инструкцию на экране). При успешной генерации Вы увидите имя ключа (в строке `gpg: ключ ... помечен как абсолютно доверенный`).

4. Добавьте в отчёт протокол выполнения команд.

5. Экспортируйте созданный ключ в текстовый *файл* (желательно в имени указывать тип ключа).

```
gpg2 --output файл --armor --export ключ
```

Вместо идентификатора ключа можно использовать имя или email (которые указывали при генерации ключей) как полностью так и частично.

Просмотрите получившийся файл. Положите его на свой веб-сайт, а в индексном файле сделайте на него ссылку. Разошлите открытый ключ товарищам по команде.

6. Чтобы получить секретный ключ, следует набрать команду

```
gpg2 --output файл --armor --export-secret-key ключ
```

7. Импортируйте к себе ключи товарищей по команде, полученные по почте или с их сайтов.

```
gpg2 --import файл  
gpg2 --allow-secret-key-import --import файл
```

Далее найдите ключ, который Вы импортировали:

```
gpg2 --list-keys
```

и наберите

```
gpg2 --edit-key ключ
```

Откроется клиент для редактирования ключа, куда можно вбивать разные команды. Напишите `trust` , из списка выберите `5 = I trust ultimately`. Потом `quit` . Теперь импортированным ключом можно пользоваться.

8. Напишите секретный текстовый файл и зашифруйте его для конкретного получателя.

```
gpg2 --recipient Получатель --encrypt файл
```

В результате файл будет зашифрован. Теперь никто, кроме получателя, не сможет его расшифровать, даже Вы сами. Попробуйте расшифровать. Чтобы расшифровать файл, необходимо использовать следующую команду:

```
gpg2 --decrypt-files файл
```

GnuPG спросит ещё Ваш секретный пароль, который Вы указали, когда создавали ключ.

9. Добавьте в отчёт содержимое своего ключа и импортированных открытых ключей (в формате ASCII).

#### Задание 4. Шифрование дисков

1. Создайте новый виртуальный диск размером 50 МБ с названием `cryptoDisk` и подключите к своей виртуальной машине.
2. Используя утилиту для работы с дисками (например, `drakdisk`), задайте для `cryptoDisk` файловую систему `ext4` с шифрованием, отформатируйте его и примонтируйте в `/mnt/cryptoDisk`.
3. Скопируйте на этот диск информацию повышенной секретности (любые файлы с указанием на цвет вашей команды).
4. Размонтируйте этот диск, выключите виртуальную машину, отсоедините диск. Обменяйтесь дисками с одногруппниками, присоедините диск, включите машину и примонтируйте диск `cryptoDisk`. Попробуйте прочитать с него данные.
5. Добавьте в отчёт скриншоты подключения и использования диска `cryptoDisk`.

#### Лабораторная работа №6

##### Укрепление защиты сети

В этой работе требуется вступить в одну двух из команд («синюю» или «красную»), выполнить настройки сети и сетевых сервисов для обеспечения улучшенной (эшелонированной) защиты и попытаться проникнуть во «вражеский стан».

##### Задание 1. Сегментация сети

Перед выполнением задания не забудьте сделать снимок виртуальной машины.

Используя первый сетевой адаптер, выполните следующие действия:

1. Проверьте тип подключения первого сетевого адаптера, — должен быть установлен **Сетевой мост**.
2. Выберите себе внутренний сетевой адрес в своей подсети: у «синих» — 10.0.1.0; у «красных» — 10.0.100.0.
3. Создайте каталог `/home/public` и сделайте его общедоступным.
4. Проверьте связь со «своими» и «чужими». Проверьте доступность сетевых сервисов («своих» и «чужих»).
5. Добавьте в отчёт конфигурацию сетевых настроек своего компьютера.

## Задание 2. Настройка файервола с помощью iptables

Перед выполнением задания не забудьте сделать снимок виртуальной машины.

Файервол, встроенный в ядро Linux, называется Netfilter, а iptables — утилита для управления этим файерволом. С помощью Netfilter можно:

- Разрешать/запрещать входящий/исходящий трафик на определенные порты по определенным протоколам (IPv4/IPv6, TCP/UDP) с указанных адресов (IP, MAC) или подсетей.
- Настраивать NAT и OpenVPN.
- Настраивать защиту от DDoS и брутфорса, ограничивать доступ в сеть конкретным приложениям, пользователям или группам.

1. Показать все правила:

```
iptables -L -n
```

В Netfilter есть «цепочки» (chains) типа INPUT, OUTPUT и FORWARD.

2. Рассмотрите следующие примеры.

Удалить все правила:

```
iptables -F
```

Изменить политику (поведение по умолчанию) цепочки:

```
iptables -P INPUT DROP
```

```
iptables -P INPUT ACCEPT
```

Запретить доступ с хоста/подсети:

```
iptables -A INPUT -s 123.45.67.89 -j DROP
```

```
iptables -A INPUT -s 123.45.0.0/16 -j DROP
```

Также можно использовать доменные имена:

```
iptables -A INPUT -s example.ru -j DROP
```

Запрет исходящих соединений:

```
iptables -A OUTPUT -d 123.45.67.89 -j DROP
```

В правилах можно использовать отрицания:

```
iptables -A INPUT ! -s 123.45.67.89 -j DROP
```

Удаление правила по его номеру в цепочке:

```
iptables -D INPUT 1
```

Удаление правила на основе того, что оно делает:

```
iptables -D INPUT -s 123.45.67.89 -j DROP
```

Опция `-p` указывает на протокол. Можно использовать `all`, `icmp`, `tcp`, `udp` или номер протокола из `/etc/protocols`.

Флаг `-sport` указывает порт, с которого был прислан пакет, а `-dport` указывает порт назначения:

```
iptables -A INPUT -p tcp --sport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Вставка (insert) правила в начало цепочки:

```
iptables -I INPUT ...
```

Или можно указать конкретную позицию:

```
iptables -I INPUT 3 ...
```

Сохранить правила:

```
iptables-save > /etc/iptables.rules
```

Восстановить правила:

```
iptables-restore < /etc/iptables.rules
```

Восстановление происходит точно так же, только флаг `-A` заменяется на флаг `-D`.

3. Создайте правила для защиты Вашего узла от чужих проникновений, оставив доступ для «своих».

Есть и более удобные инструменты для работы с `iptables`, например, есть модуль к системе `Webmin` для настроек `iptables` через веб-интерфейс (<https://localhost:10000/firewall/>).

Проверьте, что всё работает. Если да, то сохраните правила:

```
iptables-save > /etc/iptables.rules
```

4. Чтобы правила подхватывались при загрузке системы, следует создать новый файл `/etc/rc.d/init.d/iptables` (в `Rosa`, `Red Hat`, `Fedora`) или `/etc/network/if-pre-up.d/iptables` (в `Ubuntu`, `Debian`), записать в него:

```
#!/bin/sh
iptables-restore < /etc/iptables.rules
exit 0
```

и сделать его исполняемым:

```
chmod +x iptables
```

5. Добавьте в отчёт правила `iptables`.

### Задание 3. Настройка файервола с помощью `shorewall`

`Shorewall` (`Shoreline Firewall`) — инструмент для настройки файервола в `Linux`. Технически он является надстройкой над файерволом `Netfilter` ядра `Linux` и обеспечивает упрощённые методы конфигурирования данной подсистемы. Он предоставляет более высокий уровень абстракции для описания правил работы файервола.

`Shorewall` не является демоном. Правила хранятся в текстовых файлах (в каталоге `/etc/shorewall`), при запуске `shorewall` считывает свои файлы конфигурации и преобразует их в настройки, понятные `ipchains/iptables`, после чего данные настройки файервола могут действовать до перезапуска операционной системы.

`Shorewall` не имеет GUI для конфигурирования, правка конфигурационных файлов может быть произведена в любом текстовом редакторе. Есть модуль к системе `Webmin` для настроек `shorewall` через веб-интерфейс (<https://localhost:10000/shorewall/>).

Ваша задача — доработать настройки файервола `Netfilter`.

Добавьте в отчёт Ваши настройки `shorewall`.

## Лабораторная работа №7

### Политика безопасности

В этой работе Вы должны познакомиться с понятием «Политика безопасности», типовыми примерами политик и разработать собственный вариант политики безопасности для своего варианта предприятия.

Вариант предприятия можно взять из других дисциплин, где использовался проектный подход для выполнения практических заданий. При выборе предприятия надо руководствоваться, в первую очередь, хорошим знанием предметной области, а также архитектуры предприятия.

***Политика безопасности** — это совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.*

Такая трактовка, конечно, гораздо шире, чем набор правил разграничения доступа (именно это означал термин «security policy» в «Оранжевой книге» и в построенных на её основе нормативных документах других стран).

**Политика безопасности** строится на основе анализа рисков, которые признаются реальными для ИС организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

С практической точки зрения политику безопасности целесообразно рассматривать на трёх уровнях детализации.

**К верхнему уровню** можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации.

Примерный список подобных решений может включать в себя следующие элементы:

- Решение сформировать или пересмотреть комплексную программу обеспечения ИБ, назначение ответственных за продвижение программы.
- Формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей.
- Обеспечение базы для соблюдения законов и правил.
- Формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и её доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносятся управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна чётко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров по VPN или технологию BYOD). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению её в жизнь. В этом смысле политика безопасности является основой подотчётности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины.

1. Организация должна *соблюдать существующие законы*.
2. Следует *контролировать действия лиц, ответственных за выработку программы безопасности*.
3. *Необходимо обеспечить определённую степень исполнительности персонала*, а для этого нужно выработать систему поощрений и наказаний.

На верхний уровень следует выносить минимум вопросов.

Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

**Политика информационной безопасности** должна быть утверждена, издана и надлежащим образом доведена до сведения всех сотрудников организации. Она должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью.

Согласно ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью», **политика ИБ** должна включать, как минимум, следующие разделы:

- Определение информационной безопасности, её общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации.
- Изложение целей и принципов информационной безопасности, сформулированных руководством.
- Краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований.

Например, наиболее существенные политики:

1. Соответствие законодательным требованиям и договорным обязательствам;
  2. требования в отношении обучения вопросам безопасности;
  3. предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;
  4. управление непрерывностью бизнеса;
  5. ответственность за нарушения политики безопасности.
- Определение общих и конкретных обязанностей сотрудников в рамках управления ИБ, включая информирование об инцидентах нарушения ИБ.
  - Ссылки на документы, дополняющие политику ИБ, например, более детальные политики и процедуры безопасности для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

**Средний уровень политики безопасности** содержит вопросы, касающиеся отдельных аспектов ИБ, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов — отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Интернет (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров и мобильных устройств, применение пользователями неофициального программного обеспечения и т. д.

*Политика безопасности среднего уровня* должна для каждого аспекта освещать следующие темы:

**Описание аспекта** информационной безопасности. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

**Область применения** — следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?



**Позиция организации по данному аспекту** информационной безопасности. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приёма подобного ПО и т. п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отличаться.

**Роли и обязанности** — необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

**Законопослушность** — политика должна содержать общее описание запрещённых действий и наказаний за них.

**Точки контакта** — должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит определённое должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

**Политика безопасности нижнего уровня** относится к конкретным информационным сервисам. Она включает в себя два аспекта — *цели* и *правила их достижения*. Поэтому её порой трудно отделить от вопросов реализации.

Политика ИБ на этом уровне должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне.

Например, надо ответить на следующие вопросы:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удаленный доступ к сервису?

При формулировке целей политики нижнего уровня можно исходить из соображений *целостности, доступности* и *конфиденциальности*.

Её цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать.

Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жёсткие правила могут мешать работе пользователей, вероятно, их придётся часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

#### **Задание 1. Знакомство с примерами политики безопасности**

Познакомьтесь с примерами политики безопасности из открытых источников. Постарайтесь найти пример для наиболее близкой (по предметной области и архитектуре) компании.

#### **Задание 2. Разработка политики безопасности**

Создайте свой документ «Политика безопасности», взяв за основу наиболее близкий пример. Используйте известную Вам информацию о предметной области и о предприятии.

Полученный документ (в формате PDF) загрузите на Moodle.

### **3.2. Контрольные вопросы**

1. Понятие информационной безопасности. Основные составляющие информационной безопасности.
2. Основные угрозы информационной безопасности. Основные понятия.
3. Наиболее распространённые угрозы доступности.
4. Основные угрозы целостности.
5. Основные угрозы конфиденциальности.
6. Вредоносное программное обеспечение. Основные понятия.
7. Классификация вредоносных программ.
8. Способы защиты от вредоносных программ.
9. Программно-технический уровень информационной безопасности. Основные понятия.
10. Особенности современных информационных систем.
11. Архитектурная безопасность.
12. Управление доступом. Идентификация и аутентификация.
13. Авторизация.
14. Протоколы AAA.
15. Протоколирование и аудит. Основные понятия.
16. Активный аудит
17. Шифрование. Основные понятия.
18. Обеспечение конфиденциальности. Симметричное шифрование.
19. Обеспечение конфиденциальности. Асимметричное шифрование.
20. Контроль целостности. Электронная цифровая подпись. Цифровые сертификаты.
21. Административный уровень информационной безопасности. Основные понятия. Комплексная система защиты информации.
22. Политика безопасности.
23. Программа безопасности.
24. Синхронизация программы безопасности с жизненным циклом ИС.
25. Законодательный уровень информационной безопасности. Основные понятия.
26. Закон «Об информации, информатизации и защите информации».
27. Закон «О лицензировании отдельных видов деятельности».
28. Закон «Об участии в международном информационном обмене».
29. Закон «Об электронной цифровой подписи».
30. Нормативные документы.

### 3.3. Тестовые задания

Примерный перечень заданий / вопросов (образец одной попытки):

1. Сколько уровней детализации целесообразно для рассмотрения политики безопасности? Выберите один ответ:
  - 4
  - 1
  - 5
  - 3
  - 2
  - 7
2. Укажите виды блочных шифров. Выберите один или несколько ответов:
  - Покадровый шифр
  - Симметричный шифр
  - Поточковый шифр
  - Шифры подстановки
  - Асимметричный шифр
  - Шифры перестановки
3. Как называется прокси-сервер, обрабатывающий запросы от любых IP-адресов в Интернете?  
Ответ:
4. Какой метод активного аудита вызывает наименьшее число ошибок первого рода?  
Выберите один ответ:
  - метод грубой силы
  - статистический метод
  - сигнатурный метод
  - блочный метод
  - потоковый метод
5. Как называется алгоритм шифрования, для которого математически доказана его абсолютная криптографическая стойкость?  
Ответ:
6. Укажите виды нарушения статической целостности.  
Выберите один или несколько ответов:
  - кража данных
  - ввод неверных (фальшивых) данных
  - переупорядочение данных
  - дублирование данных
  - изменение данных
7. Как называется потенциальная возможность определённым образом нарушить информационную безопасность?  
Ответ:
8. Какие меры позволяют значительно повысить надёжность парольной защиты?  
Выберите один или несколько ответов:
  - ограничение доступа к файлу паролей
  - обучение пользователей
  - наложение технических ограничений

- шифрование паролей
  - шифрование файла с паролями
  - управление сроком действия паролей
  - использование программных генераторов паролей
  - ограничение числа неудачных попыток входа в систему
9. К административному уровню информационной безопасности относятся разработка законов и нормативных актов, ориентированные на людей, в области ИБ.  
Выберите один ответ:
- Верно
  - Неверно
10. Один экранирующий сервис может экранировать только один элемент.  
Выберите один ответ:
- Верно
  - Неверно
11. Как называется действие, выполняемое в рамках имеющихся полномочий, но нарушающие политику безопасности?  
Выберите один ответ:
- Протоколирование
  - Сигнатура атаки
  - Активный аудит
  - Подозрительная активность
  - Злоупотребление полномочиями
  - Аудит
12. Как называется защита от несанкционированного доступа к информации?  
Ответ:
13. Биометрия представляет собой совокупность автоматизированных методов идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик.  
Выберите один ответ:
- Верно
  - Неверно
14. Кроме удостоверяющего центра, сам пользователь может изменять информацию о себе, без нарушения целостности сертификата.  
Выберите один ответ:
- Верно
  - Неверно
15. Существует единая общепринятая классификация и номенклатура вредоносных программ.  
Выберите один ответ:
- Верно
  - Неверно
16. Многозначные пароли являются более эффективным средством, чем одноразовые пароли.  
Выберите один ответ:
- Верно
  - Неверно

17. Наиболее распространённой хеш-функцией является MD4.

Выберите один ответ:

- Верно
- Неверно

18. Как называется список, который определяет, какие субъекты могут получать доступ к конкретному объекту, и какие именно операции разрешено или запрещено этому субъекту проводить над объектом?

Ответ:

19. Частая смена программного и аппаратного обеспечения (с целью увеличения мощностей) ведёт к укреплению информационной безопасности.

Выберите один ответ:

- Верно
- Неверно

20. Как называется самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя?

Ответ:

#### 4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Практические занятия проводятся в компьютерных классах. Цель практических занятий — закрепление теоретических основ дисциплины, излагаемых в лекционном курсе, а также формирование навыков, умений и соответствующих компетенций у слушателей.

Текущий контроль осуществляется при выполнении практических работ (которые выполняются самостоятельно) — по конечному результату, с учётом вышеописанных показателей, на основе табл. 3. Результат выполнения каждой работы оценивается по 100-балльной системе.

Контроль посещения лекции осуществляется во время теоретических занятий. В случае пропуска лекции слушатель может восстановить (прочитать и написать конспект) и предъявить лекционный материал (возможно, ответив на несколько вопросов).

Промежуточная аттестация осуществляется в виде экзамена.

Для расчёта итогового балла  $B$  применяется следующая формула:

$$B = T_{\text{вход.}} + T_{\text{итог.}} + D + 0,7 \frac{\sum_{i=1}^N w_i l_i}{N} + a_i, \quad (1)$$

где  $T_{\text{итог.}} \leq 10$  — балл за итоговый тест;  $T_{\text{вход.}} \leq 10$  — балл за входной тест;  $D$  — балл за прохождение дистанционного курса (при предъявлении сертификата  $D = 10$ );  $l_i \leq 100$  — балл за  $i$ -ю выполненную слушателем работу;  $w_i$  — вес за  $i$ -ю работу (0,5 или 1);  $N$  — полное число практических работ в дисциплине;  $a_i$  — дополнительный (бонусный) балл, который слушатель может получить за активность (не более, чем 1 балл за одну лекцию).

Проведение экзамена возможно в виде тестирования, оценка за тест выражается в 100-балльной шкале. Тест состоит из вопросов по изученному теоретическому материалу, ограничение по времени: мин, метод оценивания: Последняя попытка. Слушателю разрешено сделать 3 попытки. Слушатель должен ответить на вопросы теста самостоятельно, без использования интернет-источников, учебников и иных пособий, за исключением личного конспекта слушателя. Личный конспект слушателя (допускается, как рукописный, так и электронный вариант) должен быть предъявлен преподавателю (для проверки подлинности авторства) перед проведением тестирования. Тестирование проводится в ЭУМК на [образовательном портале АлтГУ](#). Оценка выставляется автоматически по окончании теста или отведённого времени.

Окончательная оценка выводится из итогового балла на основании табл. 2.